

AVALIAÇÃO DAS MEDIDAS NECESSÁRIAS PARA ACESSO A DADOS DA DECLARAÇÃO DE APTIDÃO AO PRONAF (DAP) PELO BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL (BNDES), À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)*

*Carolina Schabbach Oliveira Ribeiro
Juliana Santos da Cruz***

RESUMO

Este parecer analisa a minuta de termo de responsabilidade a ser assinado junto ao Ministério da Agricultura, Pecuária e Abastecimento (Mapa), no intuito de permitir o acesso à base de dados da Declaração de Aptidão ao Programa Nacional de Fortalecimento da Agricultura Familiar (DAP) pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES). Ademais, são abordadas as medidas necessárias para adequação do BNDES à Lei Geral de Proteção de Dados Pessoais (Lei 13.708/2018) no tratamento dos dados pessoais compartilhados. A análise jurídica tratou dos seguintes aspectos, de acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD): a) obrigação de tratamento de dados pessoais; b) direitos dos titulares; c) adoção de medidas de segurança e sigilo dos dados; e d) governança e boas práticas. Ao longo do parecer são indicadas medidas de governança e transparência, que se estendem para além da assinatura de um termo de confidencialidade, necessárias para que o agente de tratamento, seja controlador ou operador, cumpra com os princípios que regem o tratamento de dados pessoais, tais como finalidade, adequação, transparência e minimização e outras regras previstas na LGPD.

Palavras-chave: Lei Geral de Proteção de Dados Pessoais (LGPD). Compartilhamento de dados pessoais. Governança em proteção de dados pessoais.

* Esse parecer foi elaborado com a contribuição das autoras e das seguintes advogadas do BNDES, que auxiliam o grupo de trabalho de LGPD: Andrea Paula Pontes dos Santos, mestre em Direito e Políticas Públicas pela Universidade Federal do Estado do Rio de Janeiro (UniRio); Maria da Conceição da Silva Fernandes, mestre em Direito Comparado pela Universidade da Flórida/USA e pós-graduada em Direito Societário e Mercado de Capitais pelo IBMEC; e Maria Amélia Pinheiro Pacheco Chambarelli. O conteúdo desse trabalho é de exclusiva responsabilidade dos autores, não refletindo, necessariamente, a opinião do BNDES.

** Respectivamente, advogada do BNDES, mestre em Direito na linha Empresa e Atividade Econômica pela Universidade Estadual do Rio de Janeiro (UERJ) e pós-graduada pela Pontifícia Universidade Católica do Rio Grande do Sul (PUC-RS) na área de Engenharias, na especialização MBA em Transformação Digital e Futuro dos Negócios; e advogada do BNDES.

INTRODUÇÃO

1. Trata-se de consulta ao grupo de trabalho de LGPD,¹ para avaliação de minuta de termo de responsabilidade a ser assinado junto ao Ministério da Agricultura, Pecuária e Abastecimento (Mapa), com o intuito de permitir o acesso à base de dados da Declaração de Aptidão ao Programa Nacional de Fortalecimento da Agricultura Familiar (DAP), de modo a possibilitar o monitoramento e a avaliação da efetividade do apoio do BNDES aos agricultores beneficiários.
2. A análise jurídica foi realizada estritamente sob a ótica da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei 13.709/2018) e aborda os seguintes aspectos: (i) obrigação de tratamento de dados pessoais; (ii) direitos dos titulares; (iii) adoção de medidas de segurança e sigilo dos dados; e (iv) governança e boas práticas.

I. OBRIGAÇÃO DE TRATAMENTO DE DADOS PESSOAIS

3. Inicialmente, tendo em vista que o termo de responsabilidade possibilita o compartilhamento de dados pessoais de agricultores que buscam o Pronaf, em síntese, aqueles que constam na Declaração de Aptidão ao Pronaf (DAP), o ideal em termos de governança seria que existissem cláusulas específicas regulando as obrigações tanto do BNDES como do Ministério da Agricultura, Pecuária e Abastecimento (Mapa).
4. Apesar da denominação “termo de responsabilidade”, o instrumento em análise assemelha-se a um termo de confidencialidade por tratar de questões afetas à preservação do sigilo das informações. Ademais, não objetiva regular o tratamento de dados pessoais em todos os seus aspectos, mas regulamentar o acesso aos dados em geral – pessoais ou não.
5. Contudo, a decisão sobre a necessidade de um documento com maior formalização jurídica fica a cargo do gestor dos dados pessoais, pelo menos até que sejam emitidas orientações do encarregado ou de autoridades fiscalizadoras. O gestor pode entender que o risco da ausência de regulação específica, dentro do contexto, caracteriza-se como baixo, tendo em vista as características daquele que compartilha os dados, as medidas de governança de dados que adota, bem como outros fatores casuísticos.
6. De qualquer forma, recomenda-se que durante o processo de tratamento dos dados pessoais – entendido pela LGPD, conforme o seu art. 5º, inciso X, como toda operação realizada com dados pessoais, como as que se referem “a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” (BRASIL, 2018) –, sejam observadas as medidas abaixo indicadas.
7. A utilização dos dados pessoais desses agricultores por parte do BNDES deve obedecer aos princípios elencados no art. 6º da LGPD, entre eles o da finalidade e o da adequação,

¹ Esse grupo de trabalho interno é coordenado pelo Departamento de Compliance do BNDES.

que, nesse caso específico, exigem que o BNDES receba do ministério somente aqueles dados que se mostrem essenciais para a elaboração dos documentos que permitirão a execução de consultas e estudos no âmbito das atividades de monitoramento e avaliação de efetividade do apoio realizado pelo Banco.

8. Nesse sentido, cabe ao gestor de dados avaliar quais dos dados que constam na DAP serão necessários para a avaliação e monitoramento da efetividade do apoio aos agricultores e limitar-se a receber somente esses dados, evitando, principalmente, o compartilhamento de dados pessoais sensíveis,² caso tal comportamento seja operacionalmente viável.
9. O art. 7º da LGPD, por sua vez, apresenta as hipóteses em que é possível realizar o tratamento de dados pessoais (bases legais). No caso em apreço, parece-nos que a base legal para o tratamento dos dados pessoais compartilhados pelo Mapa para a finalidade pretendida (monitoramento e avaliação de efetividade em programa de governo, Pronaf) é a execução de políticas públicas.
10. Na relação jurídica de tratamento de dados pessoais, podem existir duas partes, o controlador e o operador (agentes de tratamento). O controlador é aquele responsável pela tomada de decisões envolvendo o tratamento dos dados pessoais, sendo capaz de determinar, de maneira independente ou em conjunto com outro controlador, as finalidades da atividade de tratamento de dados pessoais, bem como os meios essenciais para a sua realização. É o controlado que define, por exemplo, quais dados serão tratados, de que forma serão coletados e o meio para essa coleta. Por sua vez, o operador é aquele que, por meio de relacionamento com terceiro que se qualifique como controlador, realiza tratamento de dados pessoais em nome e em interesse desse terceiro, de acordo com suas instruções, não sendo capaz de definir as finalidades do tratamento nem os meios essenciais para sua realização.
11. Ainda que não seja de sua alçada tomar decisões sobre o que será feito com os dados pessoais, o operador pode decidir sobre algumas questões técnicas que envolvem seu campo de atuação, como:
 - a. *sistema, método ou ferramentas utilizadas para coletar os dados pessoais;*
 - b. *meios utilizados para transferir os dados pessoais de uma organização para outra;*
 - c. *métodos utilizados para recuperar dados pessoais de determinados indivíduos;*
 - d. *maneira de garantir que o método por trás do cronograma de retenção seja respeitado;*
 - e. *meio de garantir a segurança dos dados; e*
 - f. *método de armazenamento de dados pessoais (MALDONADO; BLUM, 2020).*

2 “Art. 5º Para os fins desta Lei, considera-se: II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (BRASIL, 2018).

12. Tendo como parâmetro a legislação europeia e as situações práticas, apesar de não expressamente prevista na LGPD, a figura de cocontroladores pode existir em um caso concreto, visto que há hipóteses em que dois ou mais agentes definem e realizam, em conjunto, os propósitos e os meios de determinada atividade de tratamento de dados. A título exemplificativo, cabe destacar que a legislação europeia (GDPR) dá origem a essa expressão em seu artigo 26, prevendo “a atuação de controladores com responsabilidades conjuntas, concomitantes no tratamento de dados pessoais, determinadas mediante acordo entre as partes (contrato)” (UNIÃO EUROPEIA, 2016). Essa concomitância demonstra a possibilidade de cada uma das partes de determinar a finalidade e o tratamento que darão aos dados pessoais, de forma conjunta.
13. Ademais, de acordo com a Autoridade Nacional de Proteção de Dados (ANPD), “embora a LGPD não explicita o conceito de controladoria conjunta, é possível inferir que ele está contemplado no sistema jurídico de proteção de dados” (BRASIL, 2021, p. 12). Nesse sentido, o art. 42, § 1º, II, da referida Lei prevê a responsabilidade solidária dos controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular, o que permite concluir que em uma mesma operação de tratamento de dados pessoais pode existir mais de um controlador.
14. As principais responsabilidades e funções do controlador podem ser descritas do seguinte modo:
- i) informar o titular sobre a finalidade, forma e duração do tratamento de dados pessoal e sobre o uso compartilhado de dados pessoais;
 - ii) fazer a gestão do consentimento, quando for essa a base legal, e elaborar o Relatório de Impacto à Proteção de Dados Pessoais;
 - iii) informar o seu contato de forma clara, para que o titular possa exercer seus direitos;
 - iv) reparar danos patrimoniais, morais, individuais ou coletivos causados por violação à legislação de proteção de dados pessoais;
 - v) comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares;
 - vi) verificar se as instruções passadas foram seguidas pelo operador; e
 - vii) salvaguardar os direitos dos titulares por meio de adoção de providências, como a divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente.
15. Por sua vez, as principais responsabilidades e funções do operador são as seguintes:
- i) realizar o tratamento de dados pessoais segundo as instruções fornecidas pelo controlador;
 - ii) manter os dados pessoais protegidos de acesso não autorizado, divulgação, destruição, perda acidental ou qualquer tipo de violação de dados pessoais;
 - iii) manter registros das operações de tratamentos de dados pessoais que realizar;

- iv) auxiliar o controlador nas respostas endereçadas aos órgãos fiscalizadores, em especial a Autoridade Nacional de Proteção de Dados (ANPD); e
- v) notificar ao controlador qualquer incidente relacionado aos dados pessoais compartilhados.

16. Caracterizam-se como obrigações comuns a todos os agentes de tratamento:

- i) obedecer aos dispositivos da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) e às determinações de órgãos, entidades reguladoras/fiscalizadoras;
- ii) utilizar os dados pessoais somente para a finalidade indicada;
- iii) manter a confidencialidade e a integridade dos dados pessoais, adotando para tanto todas as medidas técnicas e administrativas necessárias;
- iv) descartar os dados ao fim do término do contrato ou mantê-los para fins estatísticos somente de forma anonimizada;
- v) adotar as técnicas organizacionais para garantir a segurança das informações compartilhadas;
- vi) manter atualizadas as técnicas de segurança da informação, bem como as medidas de proteção e segurança dos dados coletados e armazenados;
- vii) indicar o encarregado de dados pessoais; e
- viii) observar as boas práticas e padrões de governança previstos na LGPD, listados com maior detalhe no item IV - GOVERNANÇA E BOAS PRÁTICAS.

17. Em regra, ao BNDES, por ser pessoa jurídica de direito privado que explora atividade econômica, não seriam aplicáveis as regras da LGPD que se referem ao Poder Público (art. 24, caput, da LGPD).³ Contudo, como o fundamento para utilização desses dados é a execução de política pública, serão aplicáveis ao BNDES esses dispositivos (art. 24, parágrafo único), seja ele controlador ou operador na relação jurídica de compartilhamento de dados pessoais.

18. Apesar da escassez de doutrina e da ausência de jurisprudência ou orientação da ANPD sobre situações em que a mesma empresa estatal executa políticas públicas e atua em regime de competição, existem doutrinadores, tal como Fernando Menegat, que destacam que, nesses casos, a estatal deverá adotar sólido programa de governança em privacidade, recomendando a adoção das seguintes medidas:

- i. *criação de banco de dados segregados, específicos para cada modalidade de atuação da empresa;*
- ii. *consolidação de mecanismos de chinese wall e semelhantes, mediante definição de operadores e encarregados (data protection officers – DPO) para cada banco de dados, com garantia de que cada*

³ “Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei. Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo” (BRASIL, 2018).

uma das bases seja acessível apenas pelos empregados que laboram no respectivo setor da empresa;

iii. em caso de compartilhamento de dados entre diferentes setores da empresa, realização do tratamento por clean teams ou figuras semelhantes, coordenados pelos DPOs, de modo a evitar vazamentos ou apropriação indevida de dados (MENEGAT, 2020).

19. Percebe-se, então, que o termo de responsabilidade em análise adota medidas que facilitam a governança, ao vedar por parte do BNDES a disponibilização e a cessão dos dados pessoais e limitar o seu uso a uma finalidade específica, bem como ao restringir o acesso aos dados a determinados funcionários, exigindo inclusive assinatura de termo de compromisso e manutenção de sigilo que identifique o nome e o CPF daquele que tiver acesso às informações, obrigando essa pessoa a se comprometer a adotar medidas semelhantes às seguintes:
- i) manusear os dados identificados da DAP apenas para o alcance dos objetivos da pesquisa ou estudo realizado;
 - ii) manter a absoluta cautela quando da exibição de dados em tela, impressora, ou, ainda, na gravação em meios eletrônicos;
 - iii) não se ausentar do terminal sem encerrar a sessão de uso das bases, garantindo assim a impossibilidade de acesso indevido por pessoas não autorizadas; e
 - iv) manter sigilo dos dados ou informações sigilosas obtidas por força de suas atribuições, abstendo-se de revelá-los ou divulgá-los.

II. DIREITOS DOS TITULARES DE DADOS PESSOAIS

20. A Lei Geral de Proteção de Dados tem um capítulo específico sobre os direitos dos titulares (Capítulo III, arts. 17 a 22). Destacamos, ainda, o art. 9º, que, apesar de estar fora do mencionado capítulo, prevê o direito de acesso facilitado do titular às informações sobre o tratamento de seus dados, em especial sobre: finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador e a finalidade; responsabilidades dos agentes que realizarão o tratamento; e direitos do titular, com menção explícita aos direitos contidos no art. 18 da Lei. Tais informações devem ser disponibilizadas de forma clara, adequada e ostensiva, para o atendimento do princípio do livre acesso.
21. De acordo com a ANPD, “o art. 9º da LGPD estabelece os requisitos legais mínimos sobre os tipos de informações que devem ser prestadas de ofício ou mediante requerimento dos titulares” (BRASIL, 2021, p. 8). A referida autoridade pondera ainda que apesar de a LGPD não prever a obrigatoriedade de apontamento das bases legais para cumprir o princípio da transparência e o direito de acesso, como fez o GDPR em seus artigos 13 e 14, constitui boa prática prestar essa informação para que os titulares possam exercer seus direitos.
22. Como visto, o mencionado dispositivo prevê o acesso facilitado às informações sobre o tratamento de dados pessoais, o que pode ser implementado por meio de sites institucionais, políticas de privacidade, contrato, entre outros instrumentos.

23. Nesse sentido, no caso em análise, visando dar maior transparência aos titulares dos dados, recomendamos que estes sejam informados a respeito do compartilhamento de seus dados com o BNDES, inclusive no que diz respeito à finalidade do tratamento, em atendimento ao disposto no art. 9º, V, bem como aos princípios previstos no art. 6º da LGPD, dentre eles finalidade, adequação, livre acesso e transparência.
24. Merece destaque, ainda, o art. 18, que prevê que o titular dos dados pessoais tem direito de obter do controlador a qualquer momento, mediante requisição: confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD; portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD; informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e revogação do consentimento, nos termos do § 5º do art. 8º.
25. Caso não seja possível atender ao requerimento do titular, o controlador deve expor os motivos e, caso não seja o agente de tratamento, deve indicar, quando possível, o agente correto para processar o pedido, nos termos do § 4º do art. 18.

III. ADOÇÃO DE MEDIDAS DE SEGURANÇA E SIGILO DOS DADOS

26. Em relação às medidas de segurança da informação que deverão ser observadas, a LGPD criou mecanismos de proteção de dados pessoais e um capítulo específico focado na segurança da informação, sendo válido citar o artigo 46, que dispõe expressamente sobre a necessidade de todos os agentes envolvidos no tratamento de dados adotarem medidas efetivas para proteger os dados pessoais de quaisquer acessos indevidos ou incidentes de segurança:

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. [...]

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (BRASIL, 2018).

27. Deste modo, a lei deixa claro que os agentes de tratamento, seja aquele que atua como controlador ou aquele que atua como operador, ou qualquer outra pessoa que participe das fases do ciclo de vida do tratamento de dados pessoais, devem garantir a segurança da informação para proteção desses dados, sendo recomendável, inclusive, que tais agentes disponham de plano efetivo de resposta a possíveis incidentes e controles efetivos que mitiguem eventuais riscos.
28. O art. 46, § 2º, ao mencionar que as medidas de segurança, técnicas e administrativas para proteção de dados pessoais deverão ser observadas desde a fase de concepção do produ-

to ou do serviço até a sua execução, apresenta um conceito fundamental para a proteção da privacidade dos dados pessoais, de modo que as instituições devem assumir a responsabilidade pela segurança dos dados durante todo o ciclo de tratamento, observando padrões de segurança que possam garantir a confidencialidade, integridade e disponibilidade dos dados pessoais, incluindo, entre outros, métodos seguros de eliminação de dados, criptografia apropriada e métodos robustos de controle de acesso e registro.

29. Inclusive, na LGPD, a segurança e a prevenção são dois dos princípios a serem observados no tratamento de dados pessoais, destacados pelo art. 6º, incisos VII e VIII:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

VII – segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (BRASIL, 2018).

30. Em relação ao papel do BNDES, cabe ressaltar que a instituição é obrigada a cumprir várias medidas de segurança da informação necessárias à proteção dos dados pessoais de seus clientes, bem como a registrar esses dados em sistemas informatizados seguros, seja em virtude da própria LGPD, do Marco Civil da Internet (Lei 12.965, de 23 de abril de 2014) ou das normas que regulam as instituições financeiras, como as regras de sigilo bancário (Lei Complementar 105, de 10 de janeiro de 2001), e relativas ao combate à lavagem de dinheiro e ao financiamento do terrorismo (ex: Circular BCB 3978, de 23 de janeiro de 2020). Neste sentido, o BNDES possui uma robusta política de segurança da informação e, atualmente, está desenvolvendo a sua Política Corporativa de Privacidade de Dados Pessoais.⁴
31. Visando assegurar que a LGPD seja observada em sua integralidade, recomendamos que, se possível, os dados sejam eliminados ao fim do prazo de cessão – o que deve estar regulado no termo de responsabilidade ou em outro instrumento jurídico – ou, tão logo a finalidade que justificou a coleta dos dados seja cumprida, nos termos dos artigos 15 e 16 da lei.⁵ No entanto, devido à atividade que será desempenhada pelo BNDES no âmbito desse termo de responsabilidade, caso não seja possível eliminar esses dados, recomendamos que, posteriormente, estes sejam disponibilizados/divulgados somente de forma anonimizada.
32. De qualquer forma, o fato de descartar ou anonimizar os dados não descaracteriza o BNDES como agente de tratamento e não o isenta de responsabilidade em relação ao tratamento sob sua responsabilidade, sendo apenas uma boa prática recomendada pela lei ao término do tratamento dos dados, mitigando, assim, o risco de o BNDES incorrer em um possível incidente de segurança ou vazamento de dados.

4 Quando da elaboração do parecer, a Política Corporativa de Proteção de Dados estava em construção. Esse normativo foi aprovado pelo Conselho de Administração do BNDES em agosto de 2021 e trata de orientações gerais aos empregados do BNDES sobre proteção de dados, bem como da estrutura de governança interna.

5 O art. 16 da LGPD permite a conservação dos dados pessoais após o término de seu tratamento, para as seguintes finalidades: I - cumprimento de obrigação legal ou regulatória pelo controlador; II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na LGPD; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados (BRASIL, 2018).

33. Portanto, sendo viável operacionalmente a anonimização ou mesmo a eliminação dos dados, estas seriam as medidas que trariam menos exposição e riscos.
34. Além disso, dado que a lei determina que todos os agentes de tratamento devem comprovar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, incluindo a eficácia dessas medidas, destacamos ser importante o registro de que os dados realmente foram tratados nos limites estabelecidos no termo de responsabilidade e, ao final, descartados ou, então, anonimizados.
35. Por fim, é importante destacar que, nos termos do § 1º do artigo 46 da LGPD, está a cargo da ANPD e/ou órgãos reguladores setoriais definir quais serão as medidas de segurança técnicas e organizacionais adequadas para cada tipo de indústria ou negócio. A ANPD poderá dispor sobre padrões técnicos mínimos para tornar essa regra mais objetiva, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia.

IV. GOVERNANÇA E BOAS PRÁTICAS

36. Sob o aspecto da governança, o BNDES terá a obrigação de coletar e tratar os dados em proporcionalidade ao objetivo expresso no termo de responsabilidade em destaque, devendo observar medidas de segurança na utilização dos dados coletados. É importante que os dados sejam relevantes para os fins a que se destinam.
37. Portanto, no que diz respeito à governança e à privacidade, deverão ser observados os seguintes princípios da LGPD.
- i) da finalidade (art. 6º, inciso I), para que o tratamento dos dados guarde estreita relação com os propósitos informados ao titular;
 - ii) da adequação (art. 6º, inciso II) às finalidades informadas;
 - iii) da necessidade (art. 6º, inciso III), para que o tratamento esteja limitado ao mínimo necessário ao alcance das finalidades, de forma a evitar que sejam excessivos e não proporcionais às finalidades do tratamento de dados; e
 - iv) da qualidade dos dados (art. 6º, inciso V), para que seja garantida a exatidão, clareza, relevância e necessidade e para o atingimento da finalidade previamente anunciada para o tratamento.
38. Dessa forma, são medidas que se caracterizam como boas práticas: o acesso pelo menor número de pessoas aos dados pessoais, a coleta somente dos dados necessários para a finalidade a que se destina, o descarte dos dados, tão logo possível, e/ou sua anonimização, como destacado acima.
39. O compartilhamento e a cessão dos dados já são vedados pelo termo de responsabilidade, o que, caso contrário, poderia gerar a necessidade de regras mais específicas.
40. Também se recomenda que o BNDES tenha um mapeamento dos dados e do rastro de sua circulação em todas as etapas de sua utilização no âmbito interno. Essa medida facilita o cumprimento das obrigações tanto do controlador como do operador, prin-

principalmente no atendimento de demandas de autoridades fiscalizatórias ou do próprio titular dos dados.

41. Outro aspecto fundamental em termos de *accountability*, em face da LGPD, é a existência de uma política de privacidade e a indicação do encarregado pelo tratamento de dados pessoais, o DPO ou encarregado. Atualmente, o diretor responsável pela Área de *Compliance* e Riscos é o DPO indicado do BNDES.
42. Adicionalmente, destaca-se que caso entenda o gestor de dados que os mecanismos de comunicação existentes, em relação ao atendimento ao princípio da transparência, não são suficientes, deve ser avaliada adoção de medida adicional, tal como a publicação de aviso no site ou outra que entenda mais adequada, ainda que nesse caso não seja necessário o consentimento do titular de dados.

V. CONCLUSÃO

43. No que se refere ao tratamento de dados pessoais, recomenda-se a adoção das medidas acima evidenciadas, porém, destaca-se que são meramente orientativas e não dispensam outras que o gestor de dados entenda serem adequadas ao atendimento das exigências legais.

REFERÊNCIAS

BRASIL. Autoridade Nacional de Proteção de Dados Pessoais (ANPD). Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado”. Brasília, DF: 2021. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf. Acesso em: 30 ago. 2021.

BRASIL. Presidência da República. Lei 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: 18 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 4 ago. 2021.

MALDONADO, Viviane Nobrega; BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019. Disponível em: https://bibliotecadigital.tse.jus.br/xmlui/bitstream/handle/bdtse/5970/2019_maldonado_lgpd_protecao_dados.pdf?sequence=1&isAllowed=y. Acesso em: 20 set. 2021.

MENEGAT, Fernando. Tratamento de dados por empresas estatais no regime da LGPD: incertezas, desafios práticos e soluções possíveis. In: MARTINS, Ricardo Marcondes; POZZO, Augusto Neves Dal. LGPD & Administração Pública: uma análise ampla dos impactos. São Paulo: Thompson Reuters Brasil, 2020.

UNIÃO EUROPEIA. Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de Abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre Proteção de Dados). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em: 20 set. 2021.